

Curs 8

Structuri Algebraice în Informatică

• continuare curs 7

↳ cazul polinoamelor din $\mathbb{Q}[x]$

Dacă $f \in \mathbb{Q}[x]$, este ireductibil în $\mathbb{Q}[x]$.
rezultatul număratorilor coeficientilor este constant

$\exists n \in \mathbb{Z}$ astfel încât $g = xp^n \in \mathbb{Z}[x]$
 x este $\mathbb{Q}[x]$ -ul număratorilor coeficientilor din \mathbb{Q}
ai lui f .

g este ireductibil în $\mathbb{Q}[x] \Leftrightarrow f$ este ireductibil
în $\mathbb{Q}[x]$

Prop: g este ireductibil în $\mathbb{Q}[x] \Leftrightarrow g$ nu se poate scrie ca produs

de 2 polinoame
neconstanțe din
 $\mathbb{Z}[x]$

Criteriu de Eisenstein

Fix $f(x) = a_m x^m + a_{m-1} x^{m-1} + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$,

să presupunem că p este un nr. prim și că
prop. $\frac{a_m}{p} \nmid a_{m-1}, \dots, p \nmid a_1, p \nmid a_0$

$p \nmid a_0$:
Atunci f este ireductibil în $\mathbb{Q}[x]$

$$\text{Ex: } f(x) = x^5 - 2x^4 + 14x^2 \in \mathbb{Q}[x]$$

pt $p=2$ nr prim } $\begin{array}{c} \text{Gut} \\ \hline \text{Eisenstein} \end{array}$ f este ireductibil
pt $p \mid -2, 14, 2$
pt x^5

Mul di clas di resturi

Fie $f(x) = x^n + a_{m-1}x^{m-1} + \dots + a_1x + a_0 \in A[x]$
A ova inel comutativ

Pe $A[x]$ definim relația de congruență
modulo f prim: $g_1 \equiv g_2 \pmod{f} \Leftrightarrow f \mid g_1 - g_2$
Obs! $\equiv \pmod{f}$ este o relație de echivalență pe
 $A[x]$

Obs $g_1 \equiv g_2 \pmod{f} \Rightarrow g_1 \circ g_2$ daca $a_0 \neq 0$
la împărțirea primă

Pe $g \in A[x]$ $\bar{g} = \{g + hf \mid h \in A[x]\}$
Spatiu cu $A[x]/f \stackrel{\text{not}}{=} A[x]/(f)$

Prop Un sistem de reprezentanți e doar dătoare

resturilor posibili la împărțirea la f

$$\{b_0 + b_1x + \dots + b_{m-1}x^{m-1} \mid b_0, b_1, \dots, b_{m-1} \in A\}$$

Prop Fie $f_1, f_2, g_1, g_2, h \in A[x]$. So pp că
 $f_1 \equiv h \pmod{f} \wedge g_1 \equiv g_2 \pmod{f}$

Adună: $f_1 + g_1 \equiv f_2 + g_2 \pmod{f}$ $f_1 + h \equiv f_2 + h \pmod{f}$
 $f_1 \cdot g_1 \equiv f_2 \cdot g_2 \pmod{f}$ $f_1 \cdot h \equiv f_2 \cdot h \pmod{f}$

Deci pt sp. $A[x]/(f)$ putem defini 2
operatii pt reprezentantii

$$\widehat{f_1 + f_2} = \widehat{f_1} + \widehat{f_2}$$

$$\widehat{f_1 \cdot f_2} = \widehat{f_1} \widehat{f_2}$$

Prop. cu aceste operații $A[x]/(f)$ este un inel comutativ

$\widehat{0}, \widehat{1}$ termenii $\mathbb{M}[x]/(x^2 - 1)$ determinați:

\rightarrow doar $\widehat{2x+3}$ este inversabil

\rightarrow toate elem. inversabili

Ex. calculati restul din acest inel

împărțirii polinomului $g(x) = (x^3 + x + 1)^2 + 2x^2$ la
 $f(x) = x^2 + x + 1 \in \mathbb{M}[x]$

$g \bmod f$.

$$g \in \mathbb{M}[x]/(x^2 + x + 1)$$

$$g = \frac{(x^3 + x + 1)^2 + 2x^2}{x^2 + x + 1} = x^3 + x + 1 + 2x^2 = *$$

$$x^3 + x + 1 = (x^2 + x + 1)(x - 1) + (x + 2) \neq$$

$$* = \frac{(x+2)^2 + 2x^2}{x^2 + x + 1} = 3x^2 + 4x + 5 = 4(x^2 + x + 1) - x^2 = -x^2$$

Inel și iduale

Dif Inel = $(A, +, \cdot)$ mulțime nevidată

- * $(A, +)$ grup abelian \Rightarrow elem neutru la „ $+$ ”
- * (A, \cdot) monoid \Rightarrow operare cu \cdot
 - L_1 elem. neutru la „ \cdot ”
 - L_2 elem. neutru la „ $+$ ”
- * „ \cdot ” este distributiv față de „ $+$ ”
 - $a(b+c) = ab+ac$
 - $(ab)c = a(bc)$

~~sacă~~ $ab = ba \Rightarrow A$ mult comutativ $a, b, c \in A$
A inel comutativ

Corp : inel cu $1 \neq 0$ și oricărui element $\neq 0$ are invers (x^{-1} , „ \circ ”)

$U(A) = \{x \in A \mid x$ inversabil în A adică $\exists y \in A$

$$\text{cu } xy = yx = 1\}$$

Corp: $1 \neq 0$ și $U(A) = A \setminus \{0\}$

Dif: $B \subseteq A$ (inel) și numără subînăl doar

$$\forall x, y \in B : \begin{aligned} x - y &\in B \\ x \cdot y &\in B \\ 1 &\in B \end{aligned}$$

Exemplu: 1) \mathbb{N}

\downarrow
nu există

\mathbb{Z}

\downarrow
este
inel
comutativ
nu e corp

$\underbrace{B}_{\text{corpuri}} \text{ în } \mathbb{Q}$

comutativ

Exemplu: $(\mathbb{Z}_m, +, \cdot)$ este comutativ,

2) $\forall m \in \mathbb{N}$, $m \geq 2$: $(\mathbb{Z}_m, +, \cdot)$ este corp $\Leftrightarrow m$ prim

3) $\mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}\} \stackrel{\cong}{\rightarrow}$ este inel
înmulțirea lui Gauss

rezm $\mathcal{U}(\mathbb{Z}[i]) = \{1, -1, i, -i\}$

4) $\mathbb{Q}(i) = \{a+bi \mid a, b \in \mathbb{Q}\}$ este corp comutativ
(subcorp în \mathbb{C})

5) Inele de matrice

Pentru a fi comutativ

$\mathcal{M}_m(A) = \{a_{ij} \mid i, j = 1, \dots, m\}, a_{ij} \in A$

matricile de ordin n cu intrare dintr-

$(\mathcal{M}_m(A), +, \cdot)$ este inel necomutativ dacă $m \geq 2$

6) Inele de polinoame

A este comutativ $\Rightarrow (A[X], +, \cdot)$ este comutativ

7) Inelul produs: Fie A_1, A_2 două inele

Pe produsul cartezian $A_1 \times A_2 = \{a, b\}$:

a $\in A_1$ și b $\in A_2\}$ avem o strucție de inel date de operațiile efectuate pe componentă.

$$(a+b) + (a', b') = (a+a', b+b')$$

$$(a, b) \cdot (a', b') = (aa', bb')$$

Elm. neutru " + " este $(0, 0)$
" . " este $(1, 1)$

obs!

$$U(A_1 \times A_2) = U(A_1) \times U(A_2)$$

4) mulțime nul

$$A = \{0\}$$

Reguli de calcul interne înel A

1) Regula numărători: $x(-y) = (-x)y = -xy$,
+ x, yes

2) $0 \cdot a = 0 \circ 0 = 0$, $\forall a \in A$

3) Dacă $ab = ba \Rightarrow (a+b)^n = \sum_{k=0}^n c_m^k a^{m-k} b^k$
unde $c_m^k = \frac{n!}{k!(m-k)!}$

Care caracterizează înel A

$$\text{char}(A) = \begin{cases} \min \{m \mid m+1 = 0\} & \text{dacă } m \\ 0 & \text{dacă } m \end{cases}$$

$$\text{char } Z = 0$$

$$\text{char } Z_m = m$$

$$\text{char } Z[x] = 0$$

$$\text{char } Z_m[x] = m$$

Prop. docō char(A) est p nr. prim, alors

$\forall x, y \in A \quad xy = yx$ a vrm

$$(x+y)^p = x^p + y^p$$

Dém

$$(x+y)^p = c_p^0 x^p + c_p^1 x^{p-1} y + c_p^2 x^{p-2} y^2 + \dots + c_{p-1} x y^{p-1} + c_p^p y^p = x^p + y^p$$

Afirm $c_p^i \mid p$, $\forall 1 \leq i \leq p-1$

Dém: $c_p^i = \frac{p!}{(p-i)!i!} = \frac{(p-i+1)(p-i+2)\dots(p-1)p}{i!}$
 $\gcd(p, i!) = 1$

= p • (nr. natural)

Exemple: \mathbb{Z}_p (\mathbb{Z}_p , $+$, \circ) p. prim : $(a+b)^p =$

$$(a+b)^p = a^p + b^p$$

Eléments spéciaux intrinsèques à $(A, +, \circ)$

1) $x \in A$ idempotent docō $x^2 = x$

Obs: x idempotent \Leftrightarrow

2) $x \in A$ n.m. nilpotent docō $\exists n \in \mathbb{N}$ $x^n = 0$

3) $x \in A$ un divizor al lui zero doar $\Leftrightarrow y \in A$ cu
 $x \cdot y = 0$ sau $y \cdot x = 0$

Def A : o mulțime integrală nu având divizori
cu lui zero nenuli

Prop Doar A este mulțime integrală atunci
datorită $A = 0$ sau $\text{char } A = p$ prim

Def: Doar A_1, A_2 înțele, atunci se
dă: $A_1 \rightarrow A_2$ o numește morfism de mulțimi
doar:

$$f(a+b) = f(a) + f(b) \quad \forall a, b \in A_1$$

$$f(a \cdot b) = f(a) \cdot f(b)$$

$$f'(1_{A_1}) = 1_{A_2}$$

Doar în plus f bijecție spunem că este
isomorfism de mulțimi.

Prop 1) Doar fizomorfism $\Rightarrow f^{-1}$ este fizomorfism

2) Doar $f: A_1 \rightarrow A_2$ și $g: A_2 \rightarrow A_3$ morfisme
de mulțimi $\Rightarrow g \circ f$ este morfism de mulțimi

Doar f_1, f_2 izomorpisme $\Rightarrow g \circ f_1$ izomorfism

$$(g \circ f_1)^{-1} = f_1^{-1} \circ g^{-1}$$

3) Doar $f: A_1 \rightarrow A_2$ este morfism de corpuri
(adică A_1, A_2 corpuri) $\Rightarrow f$ -bijectiv $\Leftrightarrow f$ proiectiv